Journal of Number Theory **68**, 99–111 (1998)
Article No. NT972201

Orthogonal Sequences of Polynomials over Arbitrary Fields

Simon R. Blackburn*

Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom

Communicated by Alan C. Woods

Received October 28, 1996; revised September 1, 1997

Let f and g be polynomials over some field, thought of as elements of the ring of formal Laurent series. Suppose that f/g has degree 1. We investigate the set of polynomials which occur as the denominators g of badly approximable quotients f/g. Such polynomials arise in stream cipher theory (part of cryptography) as the minimal polynomials of sequences with perfect linear complexity profile. They also occur in the theory of linear cellular automata and in the analysis of certain pseudorandom number generators.

1. INTRODUCTION

Let $\mathbb{F}$ be an arbitrary field and let L be the ring of formal (one-sided) Laurent series over $\mathbb{F}$ given by

$$L = \left\{ \sum_{i=-n}^{\infty} a_i X^{-i} \mid n \in \mathbb{Z}, a_i \in \mathbb{F} \right\}.$$

We define a norm on L as follows. If $l \in L$ is non-zero, we may write $l = \sum_{i=-n}^{\infty} a_i X^{-i} \in L$ where $a_{-n} \neq 0$. In this case we define $|l| = 2^n$. If $l = 0$, we define $|l| = 0$. It is easy to verify that a theory of continued fractions exists for L, in particular we may define convergents as follows. Let $l \in L$ be such that $|l| < 1$. Let $p, q \in \mathbb{F}[X] \subseteq L$, where q is monic. We say that p/q is *a convergent for* l if for all $p', q' \in \mathbb{F}[X]$ with q' monic satisfying the inequality $|(p'/q') - l| \leqslant |(p/q) - l|$ we have that either $\deg q' > \deg q$

* The author is supported by an E.P.S.R.C. Advanced Fellowship.

0022-314X/98 $25.00

or $q' = q$. A collection of convergents can be obtained by applying the standard continued fraction algorithm.

Let $f \in \mathbb{F}[X]$ be a monic polynomial of degree d. For any polynomial $g \in \mathbb{F}[X]$ such that $\deg g < \deg f$ we say that g/f is *badly approximable* if g/f has a convergent p/q with $\deg q = i$ for all integers i such that $1 \leqslant i \leqslant d$. For a fixed monic $f \in \mathbb{F}[X]$, let m be the order of the set

$$\{g \in \mathbb{F}[X] \mid \deg g < \deg f \text{ and } g/f \text{ is badly approximable}\}.$$

We say that f has *orthogonal multiplicity m*.

The word "orthogonal" is used in deference to the following much studied situation in classical analysis [10]. Let $\mu: \mathbb{F}[X] \to \mathbb{F}$ be a linear functional. We may use μ to define a symmetric bilinear form ϕ on $\mathbb{F}[X]$ be setting $\phi(g_1, g_2) = \mu(g_1 g_2)$ for all $g_1, g_2 \in \mathbb{F}[X]$. For any positive integer i, let W_i be the subspace of $\mathbb{F}[X]$ generated by $1, X, ..., X^{i-1}$. If the form ϕ is non-degenerate on W_i for all i, there is a unique basis $f_0, f_1, ...$ for $\mathbb{F}[X]$ which is orthogonal with respect to ϕ and has the property that f_i is monic of degree i; the sequence $f_0, f_1, ...$ is known as an orthogonal sequence of polynomials. Many important sequences of polynomials (for example the Tchebycheff and Legendre polynomials) arise in this way. One may show that a monic polynomial $f \in \mathbb{F}[X]$ has positive orthogonal multiplicity if and only if f occurs as a term in some orthogonal sequence of polynomials. Indeed, if f has degree d, then the orthogonal multiplicity of f is equal to the number of choices for $f_0, f_1, ..., f_{d-1} \in \mathbb{F}[X]$ such that $f_0, f_1, ..., f_{d-1}, f$ is an initial segment of an orthogonal sequence of polynomials.

In the case when $\mathbb{F}$ is a finite field, polynomials having positive orthogonal multiplicity are of interest in several contexts. They appear in stream cipher theory (a sub-discipline of cryptography) as minimal polynomials of initial segments of sequences with perfect linear complexity profiles; see Niederreiter [8] for the equivalence between linear complexity profiles and continued fractions in the ring L. They are of relevance in the analysis (due to Niederreiter [6, 7]) of a certain class of pseudorandom number generators first proposed by Tausworthe [11]. Polynomials having positive orthogonal multiplicity have also recently been applied in cellular automata theory [2].

When $\mathbb{F}$ is infinite, every polynomial has positive orthogonal multiplicity (see Section 4). However, when $\mathbb{F}$ is finite this is not the case (for example $X(X+1) \in \mathbb{F}_2[X]$ has orthogonal multiplicity zero), so one may ask: Which polynomials have positive orthogonal multiplicity? What can be said about these multiplicities?

We prove two results. Firstly, we characterize those polynomials which have orthogonal multiplicity one:

THEOREM 1. *Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[X]$ be monic. If $\mathbb{F}$ is not of order two, then f has orthogonal multiplicity one if and only if $f = 1$. If $\mathbb{F}$ has order two, then f has orthogonal multiplicity one if and only if*

$$f = X^{e_0}(X+1)^{e_1}$$

where $\binom{e_0+e_1}{e_1} = 1 \bmod 2$.

Theorem 1 generalises two results of Niederreiter ([7, Theorem 3], [7, Proposition 1]).

Secondly, we prove that every polynomial of degree d has positive orthogonal multiplicity provided that the underlying field is sufficiently large.

THEOREM 2. *Let d be a positive integer. Let $\mathbb{F}$ be a field such that $|\mathbb{F}| \geqslant \frac{1}{2}d(d+1)$. Then every monic polynomial $f \in \mathbb{F}[X]$ of degree d has positive orthogonal multiplicity.*

These results complement those of Mesirov and Sweet [5], who show (in the terminology we use) that every non-linear irreducible polynomial over $\mathbb{F}_2$ has orthogonal multiplicity 2 (in fact, their proof also shows that any power of a non-linear irreducible polynomial over $\mathbb{F}_2$ has orthogonal multiplicity 2).

The author would like to thank Sean Murphy for his help and encouragement during the writing of this paper, and the anonymous referee for gathering supporting evidence for a conjecture in Section 5 by computer search.

2. PRELIMINARIES

Rather than working with power series $\sum_{i=1}^{\infty} s_i X^{-i}$ directly, we will work with the sequences $s_1, s_2, \ldots$ of their coefficients. For the remainder of this paper, by a sequence we will mean an infinite sequence of elements from $\mathbb{F}$, unless otherwise specified. The following lemma is easily proved.

LEMMA 1. *Let $l = \sum_{i=1}^{\infty} s_i X^{-i} \in L$ and let $f = \sum_{i=0}^{d} a_i X^i \in \mathbb{F}[X]$ be a non-zero polynomial of degree d. There exists $g \in \mathbb{F}[X]$ with* $\deg g < \deg f$ *such that $l = g/f$ if and only if*

$$\sum_{i=0}^{d} a_i s_{k+1} = 0 \qquad \text{for all integers } k \text{ such that } k \geqslant 1. \tag{1}$$

We say that a sequence $s = s_1, s_2, \ldots$ has *characteristic polynomial* f (or f is a characteristic polynomial for s) if the terms of s satisfy the recurrence (1).

The following lemma is well known. It may be proved, for example, by using the results contained in Lidl and Niederreiter [3, Section 8.6].

LEMMA 2. *A power series* $\sum_{i=1}^{\infty} s_i X^{-i}$ *has a convergent* p/q *with* $\deg q = c$ *if and only if*

$$\begin{vmatrix} s_1 & s_2 & s_3 & \cdots & s_c \\ s_2 & s_3 & s_4 & \cdots & s_{c+1} \\ s_3 & s_4 & s_5 & \cdots & s_{c+2} \\ \vdots & \vdots & \vdots & & \vdots \\ s_c & s_{c+1} & s_{c+2} & \cdots & s_{2c-1} \end{vmatrix} \neq 0. \tag{2}$$

Let $f \in \mathbb{F}[X]$ be a monic polynomial of degree d. The above lemmas imply that f has orthogonal multiplicity m if and only if there exist precisely m sequences $s_1, s_2, \ldots$ with characteristic polynomial f such that

$$\begin{vmatrix} s_1 & s_2 & s_3 & \cdots & s_c \\ s_2 & s_3 & s_4 & \cdots & s_{c+1} \\ s_3 & s_4 & s_5 & \cdots & s_{c+2} \\ \vdots & \vdots & \vdots & & \vdots \\ s_c & s_{c+1} & s_{c+2} & \cdots & s_{2c-1} \end{vmatrix} \neq 0 \qquad \text{for all} \quad c \in \{1, 2, \ldots, d\}. \tag{3}$$

The remainder of this section is concerned with characterising the set of sequences with characteristic polynomial f in a more algebraic way.

Define R_f to be the quotient $\mathbb{F}[X]/f\mathbb{F}[X]$ of $\mathbb{F}[X]$ by the principal ideal generated by f. Clearly, if we identify X with its image in R_f, an element $r \in R_f$ may be written in the form $r = b_0 + b_1 X + \cdots + b_{d-1} X^{d-1}$ for unique elements $b_0, \ldots, b_{d-1} \in \mathbb{F}$. We say a linear functional $\pi: R_f \to \mathbb{F}$ is *non-degenerate* if π is non-trivial on any non-zero ideal of R_f. For example, the map π defined by $\pi(b_0 + b_1 X + \cdots + b_{d-1} X^{d-1}) = b_{d-1}$ is non-degenerate. Now π induces a symmetric bilinear form on R_f, defined by $(r_1, r_2) \mapsto \pi(r_1 r_2)$ for all $r_1, r_2 \in R_f$. This form is non-degenerate, since for any $r_1 \in R_f \backslash \{0\}$ the functional π is non-trivial on the non-zero ideal $r_1 R_f$.

PROPOSITION 1. *Let* $f \in \mathbb{F}[X]$ *be a non-zero polynomial of degree d. Define* $R_f = \mathbb{F}[X]/f\mathbb{F}[X]$. *Let* $\pi: R_f \to \mathbb{F}$ *be a non-degenerate linear functional. Let*

$s = s_1, s_2, \ldots$ be a sequence of elements of $\mathbb{F}$. Then s has characteristic polynomial f if and only if there exists $r \in R_f$ such that

$$s_i = \pi(rX^{i-1}) \qquad \text{for} \quad i = 1, 2, \ldots. \tag{4}$$

Moreover, the element r is unique.

Proof. We may write $f = a_0 + a_1 X + \cdots + a_d X^d$ where $a_0, a_1 \cdots a_d \in \mathbb{F}$ and where $a_d \neq 0$. Any sequence $s_0, s_1, \ldots$ of the form (4) is contained in the set S of sequences with characteristic polynomial f, since for any $k \in \{1, 2, \ldots\}$

$$\sum_{i=0}^{d} a_i s_{i+k} = \sum_{i=0}^{d} a_i \pi(rX^{i+k-1}) = \pi\left(rX^{k-1} \sum_{i=0}^{d} a_i X^i\right) = 0.$$

Now the set of sequences of the form (4) forms a d dimensional subspace of the vector space of all sequences, since π is non-degenerate. But this is also the dimension of the space S. Hence the two sets are equal.

The d linear conditions on r imposed by the equality (4) for $i = 1, 2, \ldots, d$ are independent as the form induced by π is non-degenerate and the set $\{1, X, \ldots, X^{d-1}\}$ is a basis of R_f. Thus r is unique. ∎

This proposition may be regarded as a generalisation of the well known trace representation of a sequence with an irreducible characteristic polynomial [3], with R_f occupying the role of the field and π occupying the role of the trace mapping.

We remark that if $r \in R_f$ is contained in a proper ideal, say hR_f where h divides f, then the sequence of the form (4) has a characteristic polynomial of degree strictly less than d, namely f/h. In particular, we have the following.

Remark. If $s = s_1, s_2, \ldots$ is a sequence which satisfies (3) and (4), then r is not contained in any proper ideal of R_f, since otherwise s would have a characteristic polynomial of degree less than d, which would contradict (3) in the case when $c = d$.

3. PROOF OF THEOREM 1

Let $f = \sum_{i=0}^{d} a_i X^i \in \mathbb{F}[X]$ be a monic polynomial of degree d and orthogonal multiplicity one. Suppose that $\mathbb{F}$ is not of order two. By the results in Section 2, there is a unique sequence $s = s_1, s_2, \ldots$ satisfying the conditions (1) and (3). The conditions (1) and (3) are preserved under multiplication of the sequence s by a non-zero constant. Furthermore, if f is not a constant polynomial the condition (3) when $c = 1$ implies that s is

non-zero; but then this contradicts the uniqueness of s. Thus for f to have orthogonal multiplicity one we must have that $f = 1$. Furthermore, the polynomial 1 has orthogonal multiplicity one, since 0/1 is badly approximable. This shows that Theorem 1 holds for any field not of order two. For the remainder of this section, we therefore assume that $\mathbb{F}$ has order two.

Because we are working over the field of two elements, a remark of Baum and Sweet [1, p. 577] implies that the conditions (3) are equivalent to the conditions

$$\begin{aligned} s_1 &= 1 \qquad \text{and} \\ s_c + s_{2c} + s_{2c+1} &= 0 \qquad \text{for} \quad c \in \{1, 2, ..., d-1\}. \end{aligned} \tag{5}$$

Hence the orthogonal multiplicity of f is equal to the number of sequences $s_1, s_2, ...$ with characteristic polynomial f satisfying (5).

We note that Mesirov and Sweet [5] impose the extra condition that $s_d + s_{2d} + s_{2d+1} = 1$. However, this equality is implied by the conditions (1) and (5); one can see this as follows. Suppose $s = s_1, s_2, ...$ has characteristic polynomial f. Then

$$\begin{vmatrix} s_1 & s_2 & s_3 & \cdots & s_{d+1} \\ s_2 & s_3 & s_4 & \cdots & s_{d+2} \\ \vdots & \vdots & \vdots & & \vdots \\ s_{d+1} & s_{d+2} & s_{d+3} & \cdots & s_{2d+1} \end{vmatrix} = 0 \tag{6}$$

since the fact that s has a characteristic polynomial of degree d implies that the rows of the matrix in (6) are dependent. Thus, no sequence s with characteristic polynomial f can satisfy the Eqs. (5) together with $s_d + s_{2d} + s_{2d+1} = 0$, for this would contradict Eq. (6).

Mesirov and Sweet [5] mention that the methods in their paper can be used to determine the orthogonal multiplicity of any polynomial f over $\mathbb{F}_2$ in terms of the factorization of f, provided that f has positive orthogonal multiplicity. Since this result is central to our proof of Theorem 1, we give a proof of this result here.

PROPOSITION 2. *Let $f \in \mathbb{F}_2[X]$ be a polynomial having positive orthogonal multiplicity. If f has precisely k distinct non-linear irreducible factors, then the orthogonal multiplicity of f is 2^k.*

Proof. Let $f \in \mathbb{F}_2[X]$ be a polynomial having positive orthogonal multiplicity. We may write

$$f = X^{e_0}(X+1)^{e_1} \prod_{i=2}^{k+1} g_i^{e_i}$$

where $g_2, g_3, ..., g_{k+1}$ are distinct non-linear irreducible polynomials and where $e_i \geqslant 1$ for all $i \geqslant 2$.

By the remarks above, the proposition will be proved if we can show that there are precisely 2^k sequences $s_1, s_2, ...$ with characteristic polynomial f satisfying (5). Let $s'_1, s'_2, ...$ be one such sequence; such a sequence exists, since we are assuming that f has positive orthogonal multiplicity. Now, a sequence $s_1, s_2, ...$ has characteristic polynomial f and satisfies (5) if and only if the sequence $u = u_1, u_2, ...$ defined by $u_i = s_i - s'_i$ has characteristic polynomial f and satisfies the conditions

$$u_1 = 0 \qquad \text{and}$$
$$u_c + u_{2c} + u_{2c+1} = 0 \qquad \text{for} \quad c \in \{1, 2, ..., d-1\}.$$

By Proposition 1, the sequence u has characteristic polynomial f if and only if the terms of u are the form $u_i = \pi(rX^{i-1})$ for some unique $r \in R_f$. When X does not divide f, we may write $r = mX$ for a unique $m \in R_f$, as X is invertible in R_f. When X divides f, we may still write $r = mX$, though no longer uniquely; we may see this as follows. The sequence u is the difference of sequences s and s', each of which has characteristic polynomial f. By Proposition 1, there are unique elements $h, h' \in R_f$ such that

$$s_i = \pi(hX^{i-1}) \qquad \text{for all} \quad i \geqslant 1 \qquad \text{and}$$
$$s'_i = \pi(h'X^{i-1}) \qquad \text{for all} \quad i \geqslant 1.$$

By the remark after the proof of Proposition 1, we find that $h \notin XR_f$ and $h' \notin XR_f$. Hence $r \in XR_f$, since $r = h - h'$. Thus, when X divides f, we may write $r = mX$ for precisely 2 choices of $m \in R_f$.

Define an integer ε by setting

$$\varepsilon = \begin{cases} 0 & \text{if} \quad X \text{ does not divide } f \text{ and} \\ 1 & \text{otherwise.} \end{cases}$$

The above discussion shows that the orthogonal multiplicity of f is equal to $2^{-\varepsilon}$ times the number of elements $m \in R_f$ such that

$$\pi(mX) = 0 \qquad \text{and}$$
$$\pi(m(X^c + X^{2c} + X^{2c+1})) = 0 \qquad \text{for} \quad c \in \{1, 2, ..., d-1\}. \tag{7}$$

An element $m \in R_f$ satisfies (7) if and only if m is contained in the dual space to the vector space V generated by the set $\{X, X + X^2 + X^3, X^2 + X^4 + X^5, ..., X^{d-1} + X^{2d-2} + X^{2d-1}\}$. Thus there are $2^{d - \dim V}$ possibilities for m. Hence to prove the proposition, it suffices to show that $\dim V = d - k - \varepsilon$.

Let $T: R_f \to R_f$ be the linear map defined by $T(h) = h + (1+X)\,h^2$ for all $h \in R_f$. Note that $T(1) = X$ and $T(X^i) = X^i + X^{2i} + X^{2i+1}$ for any $i \geqslant 1$. Thus V is the image of T. Our final step is to determine $\dim \ker T$. An element $h \in R_f$ is contained in $\ker T$ if and only if

$$h(1 + (1+X)\,h) = 0. \tag{8}$$

To determine the solutions of this equation it suffices to compute the solutions to (8) in $R_{g_i^{e_i}}$ for $i \in \{0, 1, ..., k+1\}$ and then combine these partial solutions using the Chinese remainder theorem. It is easy to check that $h = 0$ is the only solution to (8) modulo $g_i^{e_i}$ if $g_i = (X+1)$ (or if $e_i = 0$). When $g_i \neq (X+1)$ and $e_i > 0$, it is easy to check that there are precisely two solutions to (8) modulo $g_i^{e_i}$, namely $h = 0$ and $h = (1+X)^{-1}$. Thus the number of solutions to (8) in R_f is $2^{k+\varepsilon}$. This implies that $\dim V = d - k - \varepsilon$, as required. ∎

Proof of Theorem 1. The discussion at the beginning of the section proves Theorem 1 when $\mathbb{F}$ has more than two elements, and so it suffices to consider the case when $\mathbb{F}$ has order two.

Let $f \in \mathbb{F}[X]$ be a polynomial having orthogonal multiplicity one. Proposition 2 implies that $f = X^{e_0}(X+1)^{e_1}$ for some non-negative integers e_1 and e_2 and that all polynomials of this form have multiplicity either zero or one. In order to prove Theorem 1 it therefore suffices to show that f has positive orthogonal multiplicity if and only if $\binom{e_0+e_1}{e_1} = 1 \bmod 2$.

Set $d = e_0 + e_1$, so $d = \deg f$. By making the substitution $X \mapsto X+1$ if necessary, we may assume that $e_0 < d$ (so that $e_1 \geqslant 1$).

It is easy to check, using the representation (4), that a sequence $s_1, s_2, ...$ has characteristic polynomial f if and only if the sequence $s_{e_0+1}, s_{e_0+2}, ...$ has characteristic polynomial $(X+1)^{e_1}$. Suppose that f has positive orthogonal multiplicity. Then there exists a sequence $s = s_1, s_2, ...$ with characteristic polynomial f which satisfies (5). We have that

$$1 = s_1 + \sum_{i=1}^{e_0} (s_i + s_{2i} + s_{2i+1}) = \sum_{i=e_0+1}^{2e_0+1} s_i.$$

Hence $s_{e_0+1}, s_{e_0+2}, ...$ is a sequence with characteristic polynomial $(X+1)^{e_1}$ which satisfies the equalities

$$\begin{aligned} &\sum_{i=e_0+1}^{2e_0+1} s_i = 1 \qquad \text{and} \\ &s_c + s_{2c} + s_{2c+1} = 0 \qquad \text{for all} \quad c \in \{e_0+1, ..., d-1\}. \end{aligned} \tag{9}$$

Conversely, let $s_{e_0+1}, s_{e_0+2}, \ldots$ be a sequence with characteristic polynomial $(X+1)^{e_1}$ which satisfies the equalities (9). We may define $s_1, s_2, \ldots, s_{e_0}$ to be the unique elements such that $s_c + s_{2c} + s_{2c+1} = 0$ for $c \in \{1, \ldots, e_0\}$. Then the sequence $s_1, s_2, \ldots$ has characteristic polynomial f and satisfies the equalities (5). Hence f has positive orthogonal multiplicity.

We have shown that a polynomial $f = X^{e_0}(X+1)^{e_1}$ has positive orthogonal multiplicity if and only if there exists a sequence $s_{e_0+1}, s_{e_0+2}, \ldots$ with characteristic polynomial $(X+1)^{e_1}$ satisfying the equalities (9). Using the representation (4) for sequences with a given characteristic polynomial f together with the fact that X is an invertible element in $R_{(X+1)^{e_1}}$, we may rephrase the condition for f to have positive orthogonal multiplicity as follows. We have that f has positive orthogonal multiplicity if and only if there exists $m \in R_{(X+1)^{e_1}}$ such that

$$\pi\left(m\left(\sum_{i=e_0+1}^{2e_0+1} X^i\right)\right) = 1 \qquad \text{and}$$
$$\pi(m(X^c + X^{2c} + X^{2c+1})) = 0 \qquad \text{for all} \quad c \in \{e_0+1, \ldots, d-1\}. \tag{10}$$

Let $T: R_{(X+1)^{e_1}} \to R_{(X+1)^{e_1}}$ be the linear map defined by $T(h) = h(1 + (1+X)h)$ which appeared in the proof of Proposition 2. In this situation, T is a bijection. The equalities (10) have a solution if and only if $\sum_{i=e_0+1}^{2e_0+1} X^i$ is not in the subspace generated by the set

$$\{X^c + X^{2c} + X^{2c+1} \mid c \in \{e_0+1, \ldots, d-1\}\}.$$

Now $\sum_{i=e_0+1}^{2e_0+1} X^i = T(1 + X + \cdots + X^{e_0})$ and $X^c + X^{2c} + X^{2c+1} = T(X^c)$ for all $c \geqslant 1$. So transforming our conditions by T^{-1}, and then multiplying by X^{-e_0} we find that f has positive orthogonal multiplicity if and only if

$$r = \sum_{i=0}^{e_0} X^{-i} \notin V,$$

where V is the space generated by the set $\{X, X^2, \ldots, X^{e_1-1}\}$.

As a final step, we express all the elements involved in terms of the basis $1, (X+1), \ldots, (X+1)^{e_1-1}$ of $R_{(X+1)^{e_1}}$. Now,

$$X^c = \sum_{i=0}^{c} \binom{c}{i} (X+1)^i$$

for all $c \in \{1, 2, ..., e_1 - 1\}$. This expansion always contains an even number of non-zero terms, and so

$$V = \left\{ \sum_{i=0}^{e_1-1} b_i (X+1)^i \in R_{(X+1)^{e_1}} \mid b_0, ..., b_{e_1-1} \in \mathbb{F} \text{ and } \sum_{i=0}^{e_1-1} b_i = 0 \right\}.$$

Using the convention that $\binom{-1}{0} = 1$, we may write

$$r = \sum_{i=0}^{e_0} \sum_{j=0}^{e_1-1} \binom{i+j-1}{j} (X+1)^j.$$

Thus $r \notin V$ if and only if

$$\sum_{i=0}^{e_0} \sum_{j=0}^{e_1-1} \binom{i+j-1}{j} = 1 \bmod 2.$$

But the left hand side of this equality is equal to $\binom{e_0+e_1}{e_1}$; this binomial identity corresponds to the partitioning of the e_1-subsets of $\{1, 2, ..., e_0 + e_1\}$ into those subsets which are disjoint from $\{1, 2, ..., e_0 - i\} \cup \{e_0 + e_1 - i - j + 1\}$ and contain $\{e_0 - i + 1, e_0 - i + 2, ..., e_0 + e_1 - i - j\}$. Hence f has positive orthogonal multiplicity if and only if $\binom{e_0+e_1}{e_1} = 1 \bmod 2$, as required. ∎

4. PROOF OF THEOREM 2

Let d be a positive integer, let $\mathbb{F}$ be a field such that $|\mathbb{F}| \geqslant \frac{1}{2}d(d+1)$ and let $f = \sum_{i=0}^{d} a_i X^i \in \mathbb{F}[X]$ be a monic polynomial of degree d. We wish to show that f has positive orthogonal multiplicity.

Let S be the set of sequences $s_1, s_2, ...$ with characteristic polynomial f. For any positive integer c and any $s = s_1, s_2, ... \in S$, define $M_c(s) \in \mathbb{F}$ by

$$M_c(s) = \begin{vmatrix} s_1 & s_2 & s_3 & \cdots & s_c \\ s_2 & s_3 & s_4 & \cdots & s_{c+1} \\ s_3 & s_4 & s_5 & \cdots & s_{c+2} \\ \vdots & \vdots & \vdots & & \vdots \\ s_c & s_{c+1} & s_{c+2} & \cdots & s_{2c-1} \end{vmatrix}.$$

For any positive integer c, let $V_c \subseteq S$ be the subset defined by

$$V_c = \{ s \in S \mid M_c(s) = 0 \}.$$

By the remarks in Section 2, we have that f has positive orthogonal multiplicity if and only if $\bigcup_{c=1}^{d} V_c \neq S$. We may rephrase this equivalence in the language of algebraic geometry as follows.

We may regard S as an d dimensional vector space over $\mathbb{F}$. Any element of $s \in S$ is uniquely determined by its first d terms $s_1, s_2, ..., s_d$, later terms being fixed linear combinations of these first d terms, the linear combination being determined by the recurrence associated with f. Thus for every positive integer c, we may find a polynomial $g_c \in \mathbb{F}[X_1, X_2, ..., X_d]$ which has degree at most c and is such that $M_c(s) = g_c(s_1, s_2, ..., s_d)$ for all $s = s_1, s_2, ... \in S$. When $c \in \{1, 2, ..., d\}$, we have that $g_c \neq 0$, since the sequence $s = s_1, s_2, ... \in S$ defined by

$$s_k = \begin{cases} 0 & \text{if } k \leqslant d \text{ and } k \neq c, \\ 1 & \text{if } k = c \text{ and} \\ -\sum_{i=0}^{d-1} a_i s_{k-d+1} & \text{if } k > d \end{cases}$$

has the property that $g_c(s_1, s_2, ..., s_d) = M_c(s) \neq 0$.

The set V_c is equal to the affine variety corresponding to the principal ideal in $\mathbb{F}[X_1, X_2, ..., X_d]$ generated by g_c. Define $g = g_1 g_2 \cdots g_d$. The set $\bigcup_{c=1}^{d} V_c$ is equal to the variety corresponding to the principal ideal generated by g. Clearly g is non-zero and has degree at most $\frac{1}{2}d(d+1)$. We have that $\bigcup_{c=1}^{d} V_c = S$ if and only if $g(s_1, s_2, ..., s_d) = 0$ for all $s_1, s_2, ..., s_d \in \mathbb{F}$.

Suppose that $\mathbb{F}$ has infinite order. An easy induction on d (with the fundamental theorem of algebra providing the $d = 1$ step) establishes that no non-zero polynomial $h \in \mathbb{F}[X_1, X_2, ..., X_d]$ is such that $h(s_1, s_2, ..., s_d) = 0$ for all $s_1, s_2, ..., s_d \in \mathbb{F}$. Thus g is not identically zero, and so $\bigcup_{c=1}^{d} V_c \neq S$, as required. Thus Theorem 2 follows in the case when $\mathbb{F}$ is infinite.

Suppose that $\mathbb{F}$ is finite of order n, so $n \geqslant \frac{1}{2}d(d+1)$. Analogously to the infinite case, an easy induction on d establishes that any non-zero polynomial $h \in \mathbb{F}[X_1, X_2, ..., X_d]$ is zero at $(\deg h)\, n^{d-1}$ or fewer points. Thus, whenever $n > \frac{1}{2}d(d+1)$, g is not identically zero; this proves the theorem in this case. Finally, if $n = \frac{1}{2}d(d+1)$ then $n = 3$ and $d = 2$, since n is a power of a prime; it is easy to check by hand that Theorem 2 holds in this case. ∎

5. COMMENTS

Theorem 2 shows that for large fields every polynomial of a given degree has positive orthogonal multiplicity. But Theorem 1 may be used to show that this is very far from being the case for $\mathbb{F} = \mathbb{F}_2$, as follows. When $\mathbb{F} = \mathbb{F}_2$, there are a total of 2^d monic polynomials of degree d. By Theorem 1, at most $d+1$ of these polynomials have orthogonal multiplicity one. There are precisely 2^d sequences $s_1, s_2, ...$ which have a characteristic polynomial of degree d and which satisfy the determinant conditions (3); they can be

built up as follows. The terms $s_2, s_4, ..., s_{2d}$ can be chosen arbitrarily, the terms $s_1, s_3, ..., s_{2d-1}$ are then determined by (5). There is a unique monic polynomial of degree d that is a characteristic polynomial for a sequence beginning $s_1, s_2, ..., s_{2d}$: the recursion associated with this polynomial can be used to define $s_{2d+1}, s_{2d+2}, ...$ Thus the number of sequences with a characteristic polynomial of degree d which satisfy (5) is 2^d as claimed. Since each of these sequences has a unique characteristic polynomial of degree d, there are at most $d+1+(2^d-(d+1))/2 = 2^{d-1}+\frac{1}{2}(d+1)$ polynomials of degree d over $\mathbb{F}_2$ having positive orthogonal multiplicity. Computational results (we used the Berlekamp–Massey algorithm [4] and the Zero Square Algorithm [9] in our computations) suggest that this upper bound for the number of polynomials having positive orthogonal multiplicity is far from tight, for there are large numbers of polynomials having orthogonal multiplicity 4. For example, when considering polynomials over $\mathbb{F}_2$ of degree 21, we find there are 8 of orthogonal multiplicity 1, 242888 of orthogonal multiplicity 2, 237302 of orthogonal multiplicity 4, 69266 of orthogonal multiplicity 8, 6488 of orthogonal multiplicity 16, 128 of orthogonal multiplicity 32 and 2 of orthogonal multiplicity 64. This leaves 1541070 polynomials of degree 21 which have zero orthogonal multiplicity. It would be interesting to determine the proportion of monic polynomials of degree d over $\mathbb{F}_2$ which have positive orthogonal multiplicity as $d \to \infty$.

The situation is not as regular when $\mathbb{F} \neq \mathbb{F}_2$. In particular, there seems to be no strong relationship between the orthogonal multiplicity of a polynomial f and its factorisation into irreducibles. For example, the polynomials X^4+X-1 and $X^4+X^3-X^2-X-1$ are both primitive over $\mathbb{F}_3$, but the first polynomial has orthogonal multiplicity 22 whereas the second polynomial has orthogonal multiplicity 28. Similar examples can be produced for polynomials of degree 4 over $\mathbb{F}_5$ and degree 5 over $\mathbb{F}_4$. Despite this irregular behaviour, we are yet to discover a monic polynomial over $\mathbb{F}$ which has zero orthogonal multiplicity when $\mathbb{F} \neq \mathbb{F}_2$. (Computational results by the author and the anonymous referee combine to show that all polynomials of degree at most 7 over $\mathbb{F}_3$, $\mathbb{F}_4$, $\mathbb{F}_5$ and $\mathbb{F}_7$ have positive orthogonal multiplicity, and that the same is true for degree 8 polynomials over $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_7$.) Is it the case that every monic polynomial of degree d over $\mathbb{F}$ has positive orthogonal multiplicity when $\mathbb{F} \neq \mathbb{F}_2$?

REFERENCES

1. L. E. Baum and M. M. Sweet, Badly approximable power series in characteristic 2, *Ann. of Math.* **105** (1977), 573–580.
2. K. Cattell and J. C. Muzio, Synthesis of one-dimensional linear hybrid cellular automata, *IEEE Trans. Comp. Aided Design of Integrated Systems* **15**, No. 3 (1996), 325–335.

3. R. Lidl and H. Niederreiter, "Finite Fields," Addison-Wesley, London, 1983.
4. J. L. Massey, Shift register synthesis and BCH decoding, *IEEE Trans. Inform. Theory* **15** (1969), 122–127.
5. J. P. Mesirov and M. M. Sweet, Continued fraction expansions of rational expressions with irreducible denominators in characteristic 2, *J. Number Theory* **27** (1987), 144–148.
6. H. Niederreiter, Pseudozufallszahlen und die Theorie der Gleichverteilung, *Österr. Akad. Wiss. Math.-Naturwiss. Kl.* **195** (1986), 109–138.
7. H. Niederreiter, Rational functions with partial quotients of small degree in their continued fraction expansion, *Mh. Math.* **103** (1987), 269–288.
8. H. Niederreiter, Sequences with almost perfect linear complexity profile, *in* "Advances in Cryptology: Proc. EUROCRYPT'87" (D. Chaum and W. L. Price, Eds.), Springer, Berlin, 1988, pp. 37–51.
9. N. M. Stephens, The zero square algorithm for computing linear complexity profiles, *in* "Coding and Cryptography II" (C. Mitchell, Ed.), Clarendon Press, Oxford, 1992.
10. G. Szegő, "Orthogonal Polynomials," American Math. Soc., New York, 1959.
11. R. C. Tausworthe, Random numbers generated by linear recurrences modulo two, *Math. Comp.* **19** (1965), 201–209.